

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of

**Communications Assistance for Law
Enforcement Act and Broadband Access and
Services**

ET Docket No. 04-295

RM-10865

To: The Commission

**REPLY COMMENTS OF
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

The Telecommunications Industry Association (“TIA”) hereby responds to the comments filed by the U.S. Department of Justice (“DOJ”) and other parties in this proceeding.¹

I. SCOPE OF CALEA

TIA agrees with DOJ that the Communications Assistance for Law Enforcement Act (“CALEA”) applies only to services made generally available to the public on an indiscriminate basis.² Indeed, CALEA explicitly exempts private network services.³ Further, it is equally clear,

¹ *In re Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking and Declaratory Ruling, FCC 04-187, ET Dkt. No. 04-295, RM-10865 (rel. Aug. 9, 2004) (“*CALEA NPRM*”). TIA also adopts and incorporates its previous filings in this proceeding. See Comments of the Telecommunications Industry Association (filed Nov. 8, 2004) (“*TIA Comments*”); Reply Comments of TIA and Declaration of Terri Brooks (filed April 27, 2004) (“*TIA Reply Comments on Petition*”); Comments of the Telecommunications Industry Association (filed April 12, 2004) (“*TIA Comments on Petition*”).

² See Comments of the United States Department of Justice at 14 (filed Nov. 8, 2004) (“A wire or electronic communication service that replaces local telephone exchange service and is available to a substantial portion of the public would be a ‘substantial’ replacement.”) (“*DOJ Comments*”). Also, as DOJ noted, the classic definition of common carriage includes “providing the service to the public indiscriminately.” *Id.* at 29.

³ 47 U.S.C. § 1002(b)(2)(B).

and the Commission should confirm, that “information services” are not subject to CALEA⁴ – whether they are available to the public or not.

II. STANDARDS SETTING

TIA agrees with DOJ’s new position that all widely recognized industry associations or standards bodies (not just those that are ANSI-accredited) are qualified to issue intercept standards for the purposes of CALEA’s safe harbor in section 107.⁵ As the Commission is well aware, CALEA contains no such accreditation requirement.⁶ Also, there are a variety of standards (for a variety of technologies) – in addition to those mentioned in DOJ’s comments – that industry and law enforcement have accepted as CALEA-compliant solutions, even though they were developed by non-ANSI-accredited bodies.⁷

As DOJ recognizes, the Commission should *not* attempt to use this rulemaking proceeding to determine on its own the types of call-identifying information that are “reasonably available” and therefore required to be included in a CALEA-compliant standard.⁸ TIA agrees with DOJ that deficiency petitions are the best method for resolving disputes about CALEA standards.⁹ There is no statutory basis, however, for DOJ’s proposed requirements for industry

⁴ 47 U.S.C. § 1002(b)(2)(A).

⁵ *DOJ Comments* at 54 (“[T]o ensure the ‘efficient and industry-wide implementation of the assistance capability requirements under section 103, the Commission should permit any generally recognized industry association or standard-setting body to produce a CALEA standard.’”) (citing 47 U.S.C. § 1006(a)).

⁶ CALEA merely provides that safe harbor standards are to be “adopted by an industry association or standard-setting organization.” 47 U.S.C. § 1006(a)(2).

⁷ *See, e.g., TIA Reply Comments on Petition*, Brooks Declaration at 3 (listing a number of widely used CALEA-compliant standards – and other intercept standards – produced by non-ANSI-accredited bodies).

⁸ *DOJ Comments* at 40.

⁹ *Id.* at 39.

standards-setting bodies.¹⁰ CALEA does not provide for regulatory control over the internal deliberative processes of standards bodies. Nor does CALEA allow for a standard to be evaluated on the basis of the composition of the committee that developed it. Rather, in very clear terms, CALEA delegated standards setting in the first instance to industry associations and bodies, not to the Commission or law enforcement.¹¹

Even if there were statutory authority for such rules, there is no reason to believe that Commission-crafted procedural rules are necessary or even desirable. First, TIA of course agrees that standards bodies working on CALEA should have the requisite technical expertise. This is not an issue that should be of concern to the Commission, however, as industry clearly will expend its finite resources only in standardization organizations in which such expertise resides. Second, standards bodies already typically state whether a particular standard is intended to be a CALEA standard or not.

Third, standards bodies already engage in record-keeping practices appropriate to their needs. But such record-keeping should not be regulated or required – in particular because in any deficiency proceeding, CALEA requires the Commission to review the final standard, not the deliberative process that led to it. Finally, because standards bodies operate pursuant to their own extensive internal rules and procedures, to impose additional requirements would simply be inappropriate. Adding procedural requirements where CALEA contains no such restrictions will introduce a host of new and unnecessary issues that will complicate the operation of the safe harbor process. That process should instead be focused squarely on the content of the standards.

¹⁰ DOJ proposed that industry standards bodies: (i) be recognized as representative of a segment of the telecommunications industry and that its members have the requisite technical expertise; (ii) specify which of its standards are for CALEA purposes and the technologies they cover; and (iii) maintain an adequate record of its proceedings, including a list of the capabilities considered and reasons for why certain ones were rejected. *Id.* at 55-56.

¹¹ 47 U.S.C. §§ 1006(a)(2), 1006(b).

III. TRUSTED THIRD PARTIES

TIA agrees with DOJ that trusted third parties (“TTPs”) should be neither favored nor disfavored.¹² TIA urges caution with respect to TTP solutions, however, and recommends that TTP solutions incorporate industry CALEA standards whenever possible. Such conformity will promote efficient competition among TTP providers by facilitating evaluation of competing TTP solutions.

Further, there are many ways for carriers to comply with CALEA – they may develop their own CALEA solutions, incorporate industry standards, or choose to purchase TTP solutions. Carriers may even choose to purchase from TTPs additional capabilities that law enforcement may have requested but that are not required by CALEA. In considering whether a claimed TTP solution makes certain capabilities achievable, the Commission should recognize that a number of factors may be relevant, including but not limited to whether a TTP’s technology is still in development or has actually been successfully deployed, whether it has been tested and approved by carriers for use on their complex networks, whether carriers’ networks have adequate capacity to handle the solution, whether the solution introduces delays that may reveal the existence of a wiretap, and whether it provides adequate privacy and security to carriers’ networks.

IV. COMPLIANCE DEADLINE

DOJ has introduced a new proposal for a 12-month compliance deadline in response to the Commission’s suggested 90-day compliance deadline for newly covered services. Even DOJ recognizes that the 90-day deadline would be unworkable.¹³ But TIA also disagrees with DOJ’s

¹² See *DOJ Comments* at 49.

¹³ *Id.* at 57-58. DOJ recognizes that carriers need a fair amount of time to “design solutions, hire vendors, deploy and test the intercept solutions” and notes that “unless the

new proposal for a 12-month compliance time frame. DOJ's original request for a 15-month deadline was already too short, and TIA has suggested more realistic time frames – at least 18 months for “substantial compliance” once a CALEA coverage determination is made.¹⁴ The time frames also should take into account realistic development cycles for hardware and software, which can only begin in earnest after initial standards have been developed. Similarly, time frames should take into account the time necessary to allow equipment manufacturers to work with carriers to ensure suitability of equipment-based CALEA compliance solutions for individual carriers.

V. COST OF INTERCEPTS

TIA refers the Commission to its earlier comments regarding cost recovery.¹⁵ In addition, TIA notes the concern expressed by the New York Office of the Attorney General (“NY OAG”) that the costs of implementing four “punch list” items in 1999 amounted to about \$276 million, which could result in charges of “as great as \$10,000 to \$50,000 per intercept.”¹⁶ The NY OAG complains that such charges would be “prohibitively expensive for virtually all law enforcement agencies.”¹⁷

Commission allows for a longer [compliance] timeframe . . . carriers are likely to file, *en masse*, petitions for extension.” *Id.* at 58.

¹⁴ *TIA Comments* at 8-9 (“‘substantial compliance’ would be defined as the achievement of sufficient wiretap capability so that criminals could not use the service without the content of their communications being subject to interception.”) After the 18-month substantial compliance deadline, more detailed requirements for call-identifying information would continue to be developed as provided by CALEA.

¹⁵ *Id.* at 20-24; *TIA Comments on Petition* at 25-26.

¹⁶ Comments of the Office of New York State Attorney General Eliot Spitzer at 14 (filed Nov. 8, 2004).

¹⁷ *Id.*

This admits a point that industry has been making for years. Some of the particular intercept features that have been demanded by law enforcement are very expensive – so expensive, it turns out, that law enforcement is not prepared to pay for them. NY OAG’s solution, however, is astonishing. NY OAG wants the carriers and their customers to bear this unjustified cost, even though the benefits of electronic surveillance flow to law enforcement and the public as a whole. This raises an important question: if it is not cost-effective for law enforcement (funded by the public purse) to pay for such features, how can it be cost-effective to have imposed those features in the first place, let alone to ask carriers and their customers to bear the costs?

* * *

In conclusion, TIA urges the Commission to consider fully the statements in all of its filings in this proceeding.

Respectfully submitted,



Stewart A. Baker

For Telecommunications Industry Association
Matthew J. Flanigan, President
Grant E. Seiffert, Vice President,
External Affairs and Global Policy
Derek R. Khlopin, Director, Law and
Public Policy

Of Counsel:
Stewart A. Baker
Maury D. Shenk
Emily Hancock
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036

December 21, 2004